55

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,610	02/06/2002	Zhichao Yu	60706-1250	6768

24504 7590 01/03/2006

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, LLP
100 GALLERIA PARKWAY, NW
STE 1750
ATLANTA, GA 30339-5948

EXAMINER	
MCKAY, KERRY A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/068,610	YU ET AL.	
	Examiner	Art Unit	
	Kerry McKay	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,18-29,31-38 and 47-49* is/are rejected.

7)☒ Claim(s) *10-17,30 and 39-46* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 February 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02/06/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is a non-final action in response to communications filed February 6, 2002. Claims 1-49 are pending in this action.

2. Applicant's claim to provisional application 60/266,788 filed on February 6, 2001, is noted.

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters 700, 1100, and 1200 have all been used to designate the subprocessor. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

Content of Specification

(i) Detailed Description of the Invention: See MPEP § 608.01(g). A description of the preferred embodiment(s) of the invention as required in 37 CFR 1.71. The description should be as short and specific as is necessary to describe the invention adequately and accurately. Where elements or groups of elements, compounds, and processes, which are conventional and generally widely known in the field of the invention described and their exact nature or type is not necessary for an understanding and use of the invention by a person skilled in the art, they should not be described in detail. However, where particularly complicated subject matter is involved or where the elements, compounds, or processes may not be commonly or widely known in the field, the specification should refer to another patent or readily available publication which adequately describes the subject matter.

4. The disclosure is objected to because of the following informalities:

5. The section Detailed Description of the Invention is titled Detailed Description of Drawings. Examiner recommends changing this heading to better conform to the specification contents described in MPEP § 608.01.

6. On page 1, lines 23-24, it is stated that the proposal was submitted to "the National Institute of Standards (NIS)". The correct name of this organization is the National Institute of Standards and Technology (NIST).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 22 and 32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claim 22 recites the limitation "the host memory" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim, as claim 22 is an independent claim and does not previously state a host memory.

9. Claim 32 recites the limitation "the host memory" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim, as claim 32 is an independent claim and does not previously state a host memory.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-4, 21-24, and 32-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Key et al., US Patent 6,173,386. Examiner notes that corresponding prior art terms may accompany the claim language in bracketed form.

11. Regarding claim 1, Key et al. disclose a system for enciphering information, comprising:

a first memory access unit configured to retrieve data from a host memory (figure 2, items 210 and 290, figure 3, item 700, column 8 lines 18-21);

a staggered FIFO unit (PE column) configured to perform a ShiftRow step of an Advanced Encryption Standard (AES) algorithm on the data to produce row-shifted data (figure 3, column 9, lines 34-42, 51-53, column 10, lines 50-52 column 15, lines 9-21, where it is obvious that similar modifications could made for AES that are described for DES, and Examiner interprets a column of PEs as a staggered FIFO unit);

a secondary memory access unit configured to receive the produced row-shifted data and perform a byte substitution using the row-shifted data to produce byte-substituted data (figure 3, column 9, lines 45-49, 54-61, column 15, lines 9-21, where DES also comprises S-boxes);

logic configured to receive the byte-substituted data and expand the byte-substituted data to produce manipulated data using a designated expansion algorithm (column 15, lines 9-21, where the engine comprises code for DES expansions); and

a subprocessor memory configured to receive and store the manipulated data (figure 3, column 9, lines 45-49, 54-61).

Although Key et al. do not specifically recite AES or its functions, they do state that the engine may be programmed for use in other applications, such as encryption. Key et al. further give DES, the predecessor of AES, as an example of an encryption algorithm that could be carried out by their system (column 15, lines 9-21).

12. Regarding claim 2, Key et al. disclose a system for enciphering information, comprising:

a host processor comprising a host memory, the host memory having data (figure 3, first column of PEs, column 9, lines 54-58);

a subprocessor having a subprocessor memory, the subprocessor configured to retrieve the data from the host memory and manipulate the data as the data is being loaded into the subprocessor memory (figure 3, second column of PEs, column 9, lines 45-49, 54-61).

13. Regarding claim 21, Key et al. disclose a system for enciphering information, comprising:

means for retrieving data from a host memory (figure 2, item 290);

means for performing a ShiftRow operation of an Advanced Encryption Standard (AES) algorithm on the data to produce row-shifted data (figure 3, items 400, column 9, lines 54-61, column 15, lines 9-21);

means for performing a byte substitution using the row-shifted data to produce byte-substituted data (figure 3, items 400, column 9, lines 54-61, column 15, lines 9-21);

means for expanding the byte-substituted data to produce manipulated data using a designated expansion algorithm (column 15, lines 9-21, where DES contains an expansion algorithm); and

means for storing the manipulated data (figure 3, column 15, lines 54-61).

14. Regarding claim 22, Key et al disclose a system for enciphering information, comprising:

means for retrieving data from the host memory (figure 2, item 290); and

means for manipulating the data as the data is being loaded into a subprocessor memory(figure 3, items 400, column 9, lines 54-61, column 15, lines 9-21).

15. Regarding claim 32, Key et al teach a method for enciphering information, comprising the steps of:

retrieving data from the host memory (column 8, lines 18-23); and

manipulating the data as the is being loaded into a subprocessor (PE) memory (column 9, lines 45-53).

16. As per claim 3, the system of Key et al. teaches system of claim 2. The system of Key et al., does not specifically recite that the subprocessor is configured to execute an Advanced Encryption Standard (AES) algorithm using the data; however, the system of Key et al. may be programmed for use in other applications, such as cryptography. Key et al. further name DES, the predecessor of AES, as an example of an encryption

algorithm that could be carried out by their system (column 7, lines 7-10, column 15, lines 9-21).

17. As per claim 4, the system of Key et al. teaches the system of claim 3, wherein the subprocessor comprises a first memory access unit configured to retrieve the data from a host memory (column 9, lines 45-49, 54-58).

18. As per claim 23, the system of Key et al. teaches the system of claim 22, wherein the means for manipulating the data further comprises means for executing an encryption algorithm using the data (column 15, lines 9-21). The system of Key et al., does not specifically recite the use of the AES algorithm; however, the system of Key et al. may be programmed for use in other applications, such as cryptography. Key et al. further name DES, the predecessor of AES, as an example of an encryption algorithm that could be carried out by their system (column 7, lines 7-10, column 15, lines 9-21).

19. As per claim 24, the system of Key et al. teaches the system of claim 23, wherein the means for executing the AES algorithm further comprises means for retrieving data (header) from a host memory (figure 2, item 290, column 8, lines 18-21). The system of Key et al., does not specifically recite the use of the AES algorithm; however, the system of Key et al. may be programmed for use in other applications, such as cryptography. Key et al. further name DES, the predecessor of AES, as an example of

an encryption algorithm that could be carried out by their system (column 7, lines 7-10, column 15, lines 9-21).

20. Regarding claim 33, the method of Key et al. teaches the method of claim 32, wherein the step of manipulating the data comprises the step of executing the Advanced Encryption Standard (AES) algorithm using the data (column 15, lines 9-21). Although the method of Key et al. does not specifically recite AES or its functions, it does state that the engine may be programmed for use in other applications, such as encryption. Key et al. further give DES, the predecessor of AES, as an example of an encryption algorithm that could be carried out by their system (column 15, lines 9-21).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 5-9, 18, 20, 25-29, 31, 34-38, 47, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Key et al., US Patent 6,173,386, in view of Daemen and Rijmen, "AES Proposal: Rijndael", 03/09/1999, pages 8 and 10 (hereafter referred to as Daemen et al.).

22. Regarding claim 31, Key et al. teach a method for enciphering information, comprising the steps of:

retrieving data from a host memory (figure 2, item 290, column 8, lines 18-28);

performing encryption operations on the data (column 15, lines 9-21); and

storing the manipulated data (figure 3, column 9, lines 54-61).

Key et al. do not recite AES or its operations.

Daemen et al. teach the AES algorithm and round transformations (operations) of byte substitution (ByteSub), ShiftRow, MixColumn, and AddRoundKey (page 10). Daemen et al. further provide the motivation the Rijndael algorithm was designed with resistance against all known attacks, speed and compactness on a wide range of platforms, and design simplicity (page 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to program the system of Key et al. for AES encryption because of its advantages over DES.

23. As per claim 5, the system of Key et al. teaches the system of claim 4, wherein the subprocessor further comprises a staggered FIFO unit configured to receive the retrieved data from the host memory, the staggered FIFO unit further configured to perform a step of an encryption algorithm on the data to produce row-shifted data (figure 3, column 9, lines 34-42, 51-53, column 10, lines 50-52 column 15, lines 9-21, where Examiner interprets a column of PEs as a staggered FIFO unit). The system of Key et al. does not teach AES or its operations.

Daemen et al. teach the AES algorithm and round transformations (operations) of byte substitution (ByteSub), ShiftRow, MixColumn, and AddRoundKey (page 10). Daemen et al. further provide the motivation the Rijndael algorithm was designed with resistance against all known attacks, speed and compactness on a wide range of platforms, and design simplicity (page 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to program the system of Key et al. for AES encryption because of its advantages over DES.

24. As per claim 6, the system of Key et al. and Daemen et al. teaches the system of claim 5, wherein the subprocessor further comprises a second memory access unit configured to receiver produced row-shifted data and perform a byte substitution operation on the row-shifted data using a substitution table to produce byte-substituted data (Key et al., figure 3, column 9, lines 45-49, 54-61, column 15, lines 9-21, where DES also comprises S-boxes).

25. As per claim 7, the system of Key et al. and Daemen et al. teaches the system of claim 6, wherein the subprocessor further comprises a data expansion unit configured to receive the byte-substituted data and expand the byte-substituted data to produce manipulated data using a designated expansion algorithm (Key et al., column 15, lines 9-21, where the engine comprises code for DES expansions).

26. As per claim 8, the system of Key et al. and Daemen et al. teaches the system of claim 7, wherein the subprocessor further comprises a subprocessor memory configured to receive and store the manipulated data (Key et al., column 9, lines 55-61).

27. As per claim 9, the system of Key et al. and Daemen et al. teaches the system of claim 8, wherein the subprocessor further comprises a subprocessor memory access unit configured to retrieve the stored data (Key et al., column 9, lines 45-49, 55-61).

28. As per claim 18, the system of Key et al. and Daemen et al. teaches the system of claim 6, wherein the substitution table is located in the host memory (shared memory) (Key et al., column 9, lines 10-15, column 10, lines 41-44).

29. As per claim 20, the system of Key et al. and Daemen et al. teaches the system of claim 6, wherein the substitution table is located in the subprocessor memory (Key et al., column 9, lines 10-15, column 15, lines 9-21).

30. As per claim 25, the system of Key et al. teaches the system of claim 24, further comprising means for performing a encryption functions of an encryption algorithm on the data to produce row-shifted data (figure 3, column 9, lines 54-61). The method of Key et al. does not teach performing a ShiftRow step of the AES algorithm.

Daemen et al. teach the AES algorithm and round transformations (operations) of byte substitution (ByteSub), ShiftRow, MixColumn, and AddRoundKey (page 10).

Daemen et al. further provide the motivation the Rijndael algorithm was designed with resistance against all known attacks, speed and compactness on a wide range of platforms, and design simplicity (page 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to program the system of Key et al. for the method of AES encryption because of its advantages over DES.

31. As per claim 26, the system of key et al. and Daemen et al. teaches the system of claim 25, further comprising means for performing a byte substitution operation on the row-shifted data using a substitution table to produce byte-substituted data (Key et al., figure 2, items 300 and 280, figure 3, items 400, column 9, lines 12-14, 54-61, column 15, lines 9-21).

32. As per claim 27, the system of Key et al. and Daemen et al. teaches the system of claim 26, further comprising means for expanding the byte-substituted data to produce manipulated data using a designated expansion algorithm (Key et al., figure 2, items 300 and 280, figure 3, items 400, column 9, lines 12-14, 54-61, column 15, lines 9-21).

33. As per claim 28, the system of Key et al. and Daemen et al. teaches the system of claim 27, further comprising means for storing the manipulated data (Key et al., column 9, lines 59-61).

34. As per claim 29, the system of Key et al. and Daemen et al. teaches the system of claim 28, further comprising means for retrieving the stored data (Key et al., column 9, lines 45-49, 59-65).

35. As per claim 34, the method of Key et al. teaches the method of claim 33. The method of Key et al. does not teach that the step of executing the AES algorithm comprises the step of performing a ShiftRow step of the AES algorithm on the data to produce row-shifted data.

Daemen et al. teach the AES algorithm and round transformations (operations) of byte substitution (ByteSub), ShiftRow, MixColumn, and AddRoundKey (page 10). Daemen et al. further provide the motivation the Rijndael algorithm was designed with resistance against all known attacks, speed and compactness on a wide range of platforms, and design simplicity (page 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to program the system of Key et al. for AES encryption because of its advantages over DES.

36. As per claim 35, the method of Key et al. and Daemen et al. teaches the method of claim 34, further comprising the step of performing a byte substitution operation on the row-shifted data using a substitution table to produce byte-substituted data (inherent in AES algorithm).

37. As per claim 36, the method of Key et al. and Daemen et al. teaches the method of claim 35, further comprising the step of expanding the byte-substituted data to produce manipulated data using a designated expansion algorithm (inherent in algorithm, where it is understood by Examiner that Applicant regards the MixColumn operation as an expansion).

38. As per claim 37, the method of Key et al. and Daemen et al. teaches the method of claim 36, further comprising the step of storing the manipulated data in subprocessor memory (Key et al., column 9, lines 54-61).

39. As per claim 38, the method of Key et al. and Daemen et al. teaches the method of claim 37, further comprising the step of retrieving the data stored in subprocessor memory (Key et al., column 9, lines 45-49).

40. Regarding claim 47, the method of Key et al. and Daemen et al. teaches the method of claim 35, wherein the step of performing the byte substitution operation further comprises the step of accessing a substitution table located in the host memory (shared memory) (Key et al., column 9, lines 10-15, column 10, lines 41-44).

41. As per claim 49, the method of Key et al. and Daemen et al. teaches the method of claim 35, wherein the step of performing the byte substitution operation further

comprises the step of accessing a substitution table located in the subprocessor memory (Key et al., column 9, lines 10-15, column 15, lines 9-21).

42. Claims 19 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Key et al., US Patent 6,173,386, and Daemen and Rijmen, "AES Proposal: Rijndael", 03/09/1999, pages 8 and 10 (hereafter referred to as Daemen et al.), in further view of Merkle, US Patent 5,003,597.

43. Regarding claim 19, the system of Key et al. and Daemen et al. teaches the system of claim 6. The system of Key et al. does not teach that the substitution table is configured as a hardware logic component within the subprocessor.

Merkle teaches a substitution table (S-box) configured as a hardware logic component within the subprocessor (realized in hardware)(column 1, lines 42-52). Merkle et al. further provide the motivation that substitution tables realized in hardware and operating in parallel look up multiple values simultaneously, while in software, it is done serially, making encryption and decryption cumbersome (column 1, lines 47-52). It would have been obvious to one of ordinary skill in the art, at the time of applicant's invention, to use the hardware substitution tables of Merkle with the system of Key et al. to make the byte substitution transform more efficient.

44. Regarding claim 48, the method of Key et al. and Daemen et al. teaches the method of claim 35. The method of Key et al. does not teach that the step of performing

the byte substitution operation further comprises the step of accessing a substitution table configured as a hardware logic component within the subprocessor.

Merkle teaches accessing a substitution table (S-box) configured as a hardware logic component within the subprocessor (realized in hardware)(column 1, lines 42-52). Merkle et al. further provide the motivation that substitution tables realized in hardware and operating in parallel look up multiple values simultaneously, while in software, it is done serially, making encryption and decryption cumbersome (column 1, lines 47-52). It would have been obvious to one of ordinary skill in the art, at the time of applicant's invention, to use the hardware substitution tables of Merkle in the method of Key et al. to make the byte substitution transform more efficient.

Allowable Subject Matter

45. Claims 10-17, 30, and 39-46 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

46. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Krishna et al. (US Patent 6,477,646) discloses a system and method for cryptography acceleration.

Krishna et al. (US Patent Application Publication 2003/0014627 A1) discloses a cryptography accelerator chip.

47. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kerry McKay whose telephone number is (571) 272-2651. The examiner can normally be reached on Monday-Friday, 8:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KM
12/20/2005

CEL
Primary Examiner
AU 2131
12/22/05